Attachment #34

Washington Post articles and related material

The Washington Post

Technology

Is your pregnancy app sharing your intimate data with your boss?

+ Add to list

As apps to help moms monitor their health proliferate, employers and insurers pay to keep tabs on the vast and valuable data

By Drew Harwell
April 10, 2019

Like millions of women, Diana Diller was a devoted user of the pregnancy-tracking app Ovia, logging in every night to record new details on a screen asking about her bodily functions, sex drive, medications and mood. When she gave birth last spring, she used the app to chart her baby's first online medical data — including her name, her location and whether there had been any complications — before leaving the hospital's recovery room.

But someone else was regularly checking in, too: her employer, which paid to gain access to the intimate details of its workers' personal lives, from their trying-to-conceive months to early motherhood. Diller's bosses could look up aggregate data on how many workers using Ovia's fertility, pregnancy and parenting apps had faced high-risk pregnancies or gave birth prematurely; the top medical questions they had researched; and how soon the new moms planned to return to work.

"Maybe I'm naive, but I thought of it as positive reinforcement: They're trying to help me take care of myself," said Diller, 39, an

vent planner in Los Angeles for the video game company
ctivision Blizzard. The decision to track her pregnancy had been
nade easier by the $1 a day in gift cards the company paid her to
se the app: That's "diaper and formula money," she said.

eriod- and pregnancy-tracking apps such as Ovia have climbed in
opularity as fun, friendly companions for the daunting
ncertainties of childbirth, and many expectant women check in
aily to see, for instance, how their unborn babies' size compares to
ifferent fruits or Parisian desserts.

ut Ovia also has become a powerful monitoring tool for employers
nd health insurers, which under the banner of corporate wellness
ave aggressively pushed to gather more data about their workers'
ves than ever before.

mployers who pay the apps' developer, Ovia Health, can offer
heir workers a special version of the apps that relays their health
ata — in a "de-identified," aggregated form — to an internal
mployer website accessible by human resources personnel. The
ompanies offer it alongside other health benefits and incentivize
orkers to input as much about their bodies as they can, saying the
ata can help the companies minimize health-care spending,

discover medical problems and better plan for the months ahead.

Emboldened by the popularity of Fitbit and other tracking technologies, Ovia has marketed itself as shepherding one of the oldest milestones in human existence into the digital age. By giving counseling and feedback on mothers' progress, executives said, Ovia has helped women conceive after months of infertility and even saved the lives of women who wouldn't otherwise have realized they were at risk.

But health and privacy advocates say this new generation of "menstrual surveillance" tools is pushing the limits of what women will share about one of the most sensitive moments of their lives. The apps, they say, are designed largely to benefit not the women but their employers and insurers, who gain a sweeping new benchmark on which to assess their workers as they consider the next steps for their families and careers.

'xperts worry that companies could use the data to bump up the ost or scale back the coverage of health-care benefits, or that /omen's intimate information could be exposed in data breaches r security risks. And though the data is made anonymous, experts lso fear that the companies could identify women based on ıformation relayed in confidence, particularly in workplaces /here few women are pregnant at any given time.

What could possibly be the most optimistic, best-faith reason for n employer to know how many high-risk pregnancies their mployees have? So they can put more brochures in the break ɔom?" asked Karen Levy, a Cornell University assistant professor /ho has researched family and workplace monitoring.

The real benefit of self-tracking is always to the company," Levy aid. "People are being asked to do this at a time when they're ıcredibly vulnerable and may not have any sense where that data ; being passed."

)via chief executive Paris Wallace said the company complies with rivacy laws and provides the aggregate data so employers can valuate how their workforces' health outcomes have changed over me. The health information is sensitive, he said, but could also lay a critical role in boosting women's well-being and companies' ottom lines.

"We are in a women's health crisis, and it's impacting people's lives and their children's lives," he said, pointing to the country's rising rates of premature births and maternal deaths. "But it's also impacting the folks who are responsible for these outcomes — both financially and for the health of the members they're accountable for."

The rise of pregnancy-tracking apps shows how some companies increasingly view the human body as a technological gold mine, rich with a vast range of health data their algorithms can track and analyze. Women's bodies have been portrayed as especially lucrative: The consulting firm Frost & Sullivan said the "femtech" market — including tracking apps for women's menstruation, nutrition and sexual wellness — could be worth as much as $50 billion by 2025.

Companies pay for Ovia's "family benefits solution" package on a per-employee basis, but Ovia also makes money off targeted in-app advertising, including from sellers of fertility-support supplements, life insurance, cord-blood banking and cleaning products.

An Ovia spokeswoman said the company does not sell aggregate data for advertising purposes. But women who use Ovia must consent to its 6,000-word "terms of use," which grant the company a "royalty-free, perpetual, and irrevocable license, throughout the universe" to "utilize and exploit" their de-identified personal information for scientific research and "external and internal marketing purposes." Ovia may also "sell, lease or lend aggregated Personal Information to third parties," the document adds.

Milt Ezzard, the vice president of global benefits for Activision Blizzard, a video gaming giant that earned $7.5 billion last year with franchises such as "Call of Duty" and "World of Warcraft," credits acceptance of Ovia there to a changing workplace culture where volunteering sensitive information has become more commonplace.

public education
- schools
- workplaces

In 2014, when the company rolled out incentives for workers who tracked their physical activity with a Fitbit, some employees voiced concerns over what they called a privacy-infringing overreach. But

as the company offered more health tracking — including for mental health, sleep, diet, autism and cancer care — Ezzard said women grew more comfortable with the trade-off and enticed by the financial benefits.

"Each time we introduced something, there was a bit of an outcry: 'You're prying into our lives,' " Ezzard said. "But we slowly increased the sensitivity of stuff, and eventually people understood it's all voluntary, there's no gun to your head, and we're going to reward you if you choose to do it."

"People's sensitivity," he added, "has gone from, 'Hey, Activision Blizzard is Big Brother,' to, 'Hey, Activision Blizzard really is bringing me tools that can help me out.' "

With more than 10 million users, Ovia's tracking services are now some of the most downloaded medical apps in America, and the company says it has collected billions of data points into what it calls "one of the largest data sets on women's health in the world." Alongside competitors such as Glow, Clue and Flo, the period- and pregnancy-tracking apps have raised hundreds of millions of dollars from investors and count tens of millions of users every month.

Founded in Boston in 2012, Ovia began as a consumer-facing app that made money in the tried-and-true advertising fashion of Silicon Valley. But three years ago, Wallace said, the company was approached by large national insurers who said the app could help them improve medical outcomes and access maternity data via the women themselves.

Ovia's corporate deals with employers and insurers have seen "triple-digit growth" in recent years, Wallace said. The company would not say how many firms it works with, but the number of employees at those companies is around 10 million, a statistic Ovia refers to as "covered lives."

Ovia pitches its app to companies as a health-care aid for women to better understand their bodies during a mystifying phase of life. In marketing materials, it says women who have tracked themselves with Ovia showed a 30 percent reduction in premature births, a 30 percent increase in natural conception and a higher rate of identifying the signs of postpartum depression. (An Ovia spokeswoman said those statistics come from an internal return-on-investment calculator that "has been favorably reviewed by actuaries from two national insurance companies.")

But a key element of Ovia's sales pitch is how companies can cut back on medical costs and help usher women back to work. Pregnant women who track themselves, the company says, will live healthier, feel more in control and be less likely to give birth prematurely or via a C-section, both of which cost more in medical bills — for the family and the employer.

Women wanting to get pregnant are told they can rely on Ovia's "fertility algorithms," which analyze their menstrual data and suggest good times to try to conceive, potentially saving money on infertility treatments. "An average of 33 hours of productivity are lost for every round of treatment," an Ovia marketing document says.

For employers who fund workers' health insurance, pregnancy can be one of the biggest and most unpredictable health-care expenses. In 2014, AOL chief executive Tim Armstrong defended the company's cuts to retirement benefits by blaming the high medical expenses that arose from two employees giving birth to "distressed babies."

Ovia, in essence, promises companies a tantalizing offer: lower costs and fewer surprises. Wallace gave one example in which a woman had twins prematurely, received unneeded treatments and spent three months in intensive care. "It was a million-dollar birth ... so the company comes to us: How can you help us with this?" he said.

But some health and privacy experts say there are many reasons a woman who is pregnant or trying to conceive wouldn't want to tell her boss, and they worry the data could be used in a way that puts new moms at a disadvantage.

"The fact that women's pregnancies are being tracked that closely by employers is very disturbing," said Deborah C. Peel, a

›sychiatrist and founder of the Texas nonprofit Patient Privacy Rights. "There's so much discrimination against mothers and 'amilies in the workplace, and they can't trust their employer to ıave their best interests at heart."

'ederal law forbids companies from discriminating against ›regnant women and mandates that pregnancy-related health-care :xpenses be covered in the same way as other medical conditions.)via said the data helps employers provide "better benefits, health :overage and support."

)via's soft pastels and cheery text lend a friendly air to the process ›f transmitting private health information to one's employer, and he app gives daily nudges to remind women to log their progress vith messages such as, "You're beautiful! How are you feeling oday?"

Jut experts say they are unnerved by the sheer volume and detail of lata that women are expected to offer up. Pregnant women can log letails of their sleep, diet, mood and weight, while women who are rying to conceive can record when they had sex, how they're eeling and the look and color of their cervical fluid.

ıfter birth, the app asks for the baby's name, sex and weight; who ıerformed the delivery and where; the birth type, such as vaginal ›r an unplanned C-section; how long labor lasted; whether it ncluded an epidural; and the details of any complications, such as vhether there was a breech or postpartum hemorrhage.

'he app also allows women to report whether they had a ıiscarriage or pregnancy loss, including the date and "type of loss," uch as whether the baby was stillborn. "After reporting a ıiscarriage, you will have the option to both reset your account nd, when you're ready, to start a new pregnancy," the app says.

"We're their companion throughout this process and want to ... provide them with support throughout their entire journey," Ovia spokeswoman Sarah Coppersmith said.

Much of this information is viewable only by the worker. But the company can access a vast range of aggregated data about its employees, including their average age, number of children and current trimester; the average time it took them to get pregnant; the percentage who had high-risk pregnancies, conceived after a stretch of infertility, had C-sections or gave birth prematurely; and the new moms' return-to-work timing.

Companies can also see which articles are most read in Ovia's apps, offering them a potential road map to their workers' personal questions or anxieties. The how-to guides touch on virtually every aspect of a woman's changing body, mood, financial needs and lifestyle in hyper-intimate detail, including filing for disability, tracking bodily aches and discharges, and suggestions for sex positions during pregnancy.

"We are crossing into a new frontier of vaginal digitalization," wrote Natasha Felizi and Joana Varon, who reviewed a group of menstrual-tracking apps for the Brazil-based tech activist group Coding Rights.

Ovia data is viewable by the company, their insurers and, in the case of Activision Blizzard and other self-insured companies, the third-party administrators that process women's medical claims.

Ovia says it is compliant with government data-privacy laws such as the Health Insurance Portability and Accountability Act, or HIPAA, which sets rules for sharing medical information. The company also says it removes identifying information from women's health data in a way that renders it anonymous and that it requires employers to reach a certain minimum of enrolled users

efore they can see the aggregated results.

ut health and privacy experts say it's relatively easy for a bad actor o "re-identify" a person by cross-referencing that information with ther data. The trackers' availability in companies with few regnant women on staff, they say, could also leave the data ulnerable to abuse. Ovia says its contract prohibits employers rom attempting to re-identify employees.

zzard, the benefits executive at Activision Blizzard, said offering regnancy programs such as Ovia helps the company stand out in a ompetitive industry and keep skilled women in the workforce oming back. The company employs roughly 5,000 artists, evelopers and other workers in the United States.

I want them to have a healthy baby because it's great for our usiness experience," Ezzard said. "Rather than having a baby ho's in the neonatal ICU, where she's not able to focus much on ork."

efore Ovia, the company's pregnant employees would field eriodic calls from insurance-company nurses who would ask bout how they were feeling and counsel them over the phone. hifting some pregnancy care to an app where the women could ive constant check-ins made a huge difference: Nearly 20 women ho had been diagnosed as infertile had become pregnant since the ompany started offering Ovia's fertility app, Ezzard said.

oughly 50 "active users" track their pregnancies at any given time, nd the average employee records more than 128 health data oints a month, Ezzard said. They also open the app about 48 times month, or more than once a day.

zzard said that the company maintains strict controls on who can eview the internal aggregated data and that employees' medical

claims are processed at a third-party data warehouse to help protect their privacy. The program, he added, is already paying off: Ovia and the other services in its "well-being platform" saved the company roughly $1,200 per employee in annual medical costs.

Health experts worry that such data-intensive apps could expose women to security or privacy risks. The ovulation-tracking app Glow updated its systems in 2016 after Consumer Reports found that anyone could access a woman's health data, including whether she'd had an abortion and the last time she'd had sex, as long as they knew her email address. Another Ovia competitor, Flo, was found to be sending data to Facebook on when its users were having their periods or were trying to conceive, according to tests published in February in the Wall Street Journal. Ovia says it does not share or sell data with social media sites.

The company says it does not do paid clinical trials but provides data to researchers, including for a 2017 study that cited Ovia data from more than 6,000 women on how they chose their obstetricians. But even some researchers worry about ways the information might be used.

"As a clinician researcher, I can see the benefit of analyzing large data sets," said Paula M. Castaño, an obstetrician-gynecologist and associate professor at Columbia University who has studied menstrual-tracking apps. But a lot of the Ovia data given to employers, she said, raises concerns "with their lack of general clinical applicability and focus on variables that affect time out of work and insurance utilization."

Ovia says its "fertility algorithms," which analyze a woman's data and suggest when she would have the best chance of getting pregnant, have helped 5 million women conceive. But the claim is impossible to prove: Research into similar promises from other

ıpps has suggested there were other possible explanations, ncluding the fact that the women were motivated enough to use a ɔeriod-tracking app in the first place.

The coming years, however, will probably see companies pushing for more pregnancy data to come straight from the source. The Israeli start-up Nuvo advertises a sensor band strapped around a woman's belly that can send real-time data on fetal heartbeat and uterine activity "across the home, the workplace, the doctor's office and the hospital." Nuvo executives said its "remote pregnancy monitoring platform" is undergoing U.S. Food and Drug Administration review.

Diller, the Activision Blizzard employee, said she was never troubled by Ovia privacy worries. She loved being able to show her friends what size pastry her unborn daughter was and would log her data every night while lying in bed and ticking through her other health apps, including trackers for food, sleep and mindfulness."

When she reported the birth in Ovia, the app triggered a burst of virtual confetti and then directed her to download Ovia's parenting app, where she could track not just her health data, but her newborn daughter's, too. It was an easy decision. On the app's home screen, she uploaded the first photo of her newly expanded family.

Drew Harwell

Drew Harwell is a technology reporter for The Washington Post covering artificial intelligence and the algorithms changing our lives. He joined The Post in 2014 and has covered national business and the Trump companies. Follow

Pregnancy-Tracking Apps Pose Challenges for Employees

Friday, April 26, 2019

As more companies embrace health-tracking apps to encourage healthier habits and drive down healthcare costs, some employees are becoming uncomfortable with the amount and types of data the apps are sharing with their employers, insurance companies and others.

This is especially true for apps that track fertility and pregnancy. As the *Washington Post* recently reported, these apps collect huge amounts of personal health information, and are not always transparent about who has access to it. The digital rights organization Electronic Frontier Foundation even published a paper in 2017 titled *The Pregnancy Panopticon* detailing the security and privacy issues with pregnancy-tracking apps. Employers can also pay extra for some pregnancy-tracking apps to provide them with employees' health information directly, ostensibly to reduce health care spending and improve the company's ability to plan for the future.

Given the documented workplace discrimination against women who are pregnant or planning to become pregnant, users may worry that the information they provide the apps could impact employment options or treatment by colleagues and managers. Pregnancy-tracking apps also collect infinitely more personal data than traditional health-tracking apps and devices like step-counters or heart rate monitors. This can include everything from what medications users are taking and when they are having sex or their periods, to the color of their cervical fluid and their doctors' names and locations.

Citing discomfort with providing this level of information, the *Washington Post* reported some women have even taken steps to obscure their personal details when using the apps, for fear that their employers, insurance companies, health care providers or third parties may have access to their data and could use it against them in some way. They use fake names or fake email addresses and only give the apps select details or provide inaccurate information. Fearing the invasion of their newborn children's privacy, some have even chosen not to report their children's births on the apps, despite this impacting their ability to track their own health and that of their newborn on the app.

Like many other apps or online platforms, it may be difficult to parse out exactly what health-tracking apps are doing with users' information and what you are agreeing to when you sign up. When employers get involved, these issues get even more difficult. By providing incentives—either in the form of tangible rewards like cash or gift cards, or intangible benefits such as looking like a team player—companies may actually discourage their employees from looking closely at the apps' terms of use or other key details they need to fully inform the choice to participate or not.

While getting more information about employees' health may offer ways to improve a workforce's health and reduce treatment costs, companies encouraging their employees to use these apps are also opening themselves up to risks. As noted above, apps are not always transparent as to what information they are storing and how. Depending on the apps' security practices, employees' data may be susceptible to hacking or other misuse by third-party or malicious actors. For example, in January 2018, fitness-tracking app Strava released a map of users' activity that inadvertently exposed sensitive information about military personnel's locations, including in war zones. Given the kinds of personal details that some apps collect, health app data could also put users at risk of identity theft or other types of fraud.

Tracking, storing, and using workers' personal health information also exposes employers and insurance companies to a number of risks and liabilities, including third-party data storage vulnerabilities and data breaches. This is especially important in places governed by stringent online data protection regulations like the European Union's General Data Protection Regulation (GDPR). In addition to the risks of reputation damage,

ARTICLE BY
Adam Jacobson

Risk and Insurance Management Society, Inc. (RIMS)
Risk Management Monitor

RISK MANAGEMENT
RISK MONITOR

Labor & Employment
Communications, Media & Internet
Health Law & Managed Care
All Federal

PRINTER-FRIENDLY
EMAIL THIS ARTICLE
DOWNLOAD PDF
REPRINTS & PERMISSIONS

RELATED ARTICLES

New Podcast: Whose Data Is It Anyway? Collaboration in Digital Health

Is Your Employer Worksite Medical Clinic a Group Health Plan?

The Bubbler - Employment Law Compliance February 2019

Economic Trends and Your Board [Podcast]

TRENDING LEGAL ANALYSIS

Successfully Navigating Export Controls in a Fast Changing Regulatory and Political Environment
By Womble Bond Dickinson (US) LLP

UK Government Announces Review into Private Sector IR35 Rules
By Proskauer Rose LLP

UK Government Announces Review into Private Sector IR35 Rules
By Proskauer Rose LLP

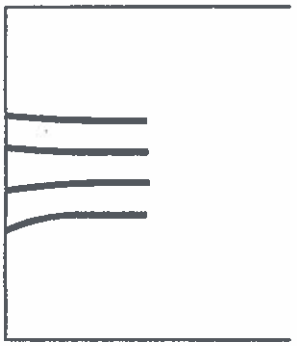
New Antidumping and Countervailing Duty Petitions on Wood Mouldings and Millwork Products from Brazil and China
By Drinker Biddle & Reath LLP

New Antidumping and Countervailing Duty Petitions on Wood Mouldings and Millwork Products from Brazil and China
By Drinker Biddle & Reath LLP

Department of Homeland Security Warns of Cyber-attacks by Iran
By Robinson & Cole LLP

companies that are breached or otherwise expose employees' personal information could face significant regulatory fines.

People using health-tracking apps, especially fertility-related apps, should weigh the costs and benefits of disclosing personal information against how apps and others are using this information. Companies who encourage their employees to use these apps and collect their personal health details should also be as transparent as possible about how they are using it, and implement measures to protect workers' personal data to the fullest extent possible and ensure that managers are not using this data to discriminate against workers.



ABOUT THIS AUTHOR

Adam Jacobson

Adam Jacobson is associate editor of the Risk Management Monitor and Risk Management magazine.

www.rmmagazine.com
212-655-5919
www.rmmagazine.com

The Washington Post
Democracy Dies in Darkness

These apps may have told Facebook about the last time you had sex

A new report found that period-tracking apps Maya and MIA Fem shared intimate information with Facebook.

By **Marie C. Baca**

September 17, 2019 at 3:21 p.m. EDT

Editor's Note: A sentence originally published in this story used language similar to what appeared in a BuzzFeed story on the same subject. The story has been revised to eliminate the similarities.

Your best friend may not know when you last had sex, but it's possible that Facebook does.

At least two menstruation-tracking apps, Maya and MIA Fem, were sharing intimate details of users' sexual health with Facebook and other entities, according to a new report from Britain-based privacy watchdog Privacy International. In some cases, those details, which are self-recorded by users in the app, included when a user last had sex, the type of contraception used, her mood and whether she was ovulating.

The findings raise questions about the security of our most private information in an age where employers, insurers and advertisers can use data to discriminate or target certain categories of people.

The information was shared with the social media giant via the Facebook Software Development Kit, a product that allows developers to create apps for specific operating systems, track analytics and monetize their apps through Facebook's advertising network. Before users could even agree to the apps' privacy policies, both Maya and MIA started sharing some data as soon they were opened, according to Privacy International.

Facebook spokesman Joe Osborne said advertisers did not have access to the sensitive health information shared by these apps. In a statement, he said Facebook's ad system "does not leverage information gleaned from people's activity across other apps or websites" when advertisers choose target users by interest. BuzzFeed first reported the news.

Period- and pregnancy-tracking apps such as Maya and MIA have climbed in popularity as fun, friendly companions that provide insights into the often daunting world of fertility and pregnancy. They can also be used to track sexual health more generally, moods and other intimate data. But many apps aren't subject to the same rules as most health data.

That has raised privacy concerns as some of the apps have come under scrutiny as powerful monitoring tools for employers and health insurers, which have aggressively pushed to gather more data about their workers' lives than ever before under the banner of corporate wellness. Plus, it appears the data could be shared more broadly than many users recognize, as flagged by the Privacy International study.

Several period- and pregnancy-tracking apps have been called out for sharing health data with women's employers and insurance companies, as well as for security flaws that reveal intimate information. As a result, many women say they've devised strategies to use the apps without revealing all of their most sensitive information. Among those strategies: using fake names, documenting only scattered details and even inputting incorrect data.

Users and experts alike worry that the data could be exposed in security breaches, or used by employers and insurance companies to discriminate against women by increasing their premiums or not offering them leadership positions.

Deborah C. Peel, a psychiatrist and founder of the nonprofit Patient Privacy Rights, said people expect that their health data will be protected by the same laws that protect their health information in a doctors office, but that many apps aren't subject to the same rules.

"Most people would want to make their own decisions about what's known about their sex life, about whether it's shared or not," said Peel. "Right now we have no ability to do that."

Facebook, the world's largest social media platform with 1.2 billion daily users, is asking users to trust it with more and more sensitive information than at any time in the past. Last week, the company launched Facebook Dating in the United States, a matchmaking service that suggests potential love interests to users based on preferences, interests and Facebook activity.

At the same time, Facebook has come under fire in recent years for multiple scandals involving misinformation, fake accounts and breaches of trust. That includes the 2018 revelation from a whistleblower that Facebook had allowed political consultancy firm Cambridge Analytica to improperly access data from millions of users. In that case, the data was harvested through a third-party quiz app.

In a Facebook statement included in the report, the company said its terms of service prohibit app developers from sharing health or sensitive data, and that it has been in contact with Maya and MIA to notify them of a possible violation of those terms. Facebook also said that while it has systems in place to automatically detect and delete information like Social Security numbers and passwords from the information shared by apps, the company is "looking at ways to improve our system/products to detect and filter out more types of potentially sensitive data."

Plackal Tech, which developed Maya, said in its statement to Privacy International that it would remove the Facebook Software Development Kit from a new version of its service. There was no published response from Mobapp Development, the company behind MIA, and the company did not have an immediate comment.

AD

https://www.washingtonpost.com/business/2019/10/14/colleges-quietly-rank-prospective-students-based-their-personal-data/

To learn more about prospective students, admissions officers at the University of Wisconsin-Stout turned to a little-known but increasingly common practice: They installed tracking software on their school website.

When one student visited the site last year, the software automatically recognized who she was based on a piece of code, called a cookie, which it had placed on her computer during a prior visit. The software sent an alert to the school's assistant director of admissions containing the student's name, contact information and details about her life and activities on the site, according to internal university records reviewed by The Washington Post. The email said she was a graduating high school senior in Little Chute, Wis., of Mexican descent who had applied to UW-Stout.

Some colleges are tracking students before they even apply

The admissions officer also received a link to a private profile of the student, listing all 27 pages she had viewed on the school's website and how long she spent on each one. A map on this page showed her geographical location, and an "affinity index" estimated her level of interest in attending the school. Her score of 91 out of 100 predicted she was highly likely to accept an admission offer from UW-Stout, the records showed.

Colleges are collecting more data about prospective students than ever before — part of an effort, administrators say, to make better predictions about which students are the most likely to apply, accept an offer and enroll. Records reviewed by The Post show that at least 44 public and private universities in the United States work with outside consulting companies to collect and analyze data on prospective students, by tracking their Web activity or formulating predictive scores to measure each student's likelihood of enrolling.

The practices may raise a hidden barrier to a college education for underprivileged students. While colleges have used data for many years to decide which regions and high schools to target their recruiting, the latest tools let

administrators build rich profiles on individual students and quickly determine whether they have enough family income to help the school meet revenue goals.

The Post identified colleges with data operations by reviewing the customer lists of two top admissions consulting firms: Capture Higher Ed and Ruffalo Noel Levitz. The Post interviewed admissions staffers at 23 colleges, examined contracts and emails obtained from 26 public universities through open-records laws, and used a Web privacy tool to confirm the presence of Capture Higher Ed's tracking software on the websites of 33 universities.

Records and interviews show that colleges are building vast repositories of data on prospective students — scanning test scores, Zip codes, high school transcripts, academic interests, Web browsing histories, ethnic backgrounds and household incomes for clues about which students would make the best candidates for admission. At many schools, this data is used to give students a score from 1 to 100, which determines how much attention colleges pay them in the recruiting process.

Scoring and tracking are popular at schools that are struggling to survive. Faced with shrinking sources of funding and growing competition for high school graduates, cash-strapped colleges are experimenting with new ways to identify and attract students who can afford to pay tuition, said Lloyd Thacker, a former admissions counselor and founder of the Education Conservancy, a nonprofit research group.

Post Reports: Reporter Doug MacMillan on why colleges are starting to track prospective applicants

"An admission dean is more and more a businessperson charged with bringing in revenue," Thacker said. "The more fearful they are about survival, the more willing they are to embrace new strategies."

Admissions consulting companies charge schools tens of thousands of dollars a year to collect and analyze the data of millions of students. In emails reviewed by The Post, employees of Louisville-based Capture Higher Ed urged school administrators to hand over all data they felt comfortable sharing.

"We love data, so the more the merrier," one of Capture's consultants wrote in a 2017 email to the admissions director at UW-Stout.

Capture Higher Ed spokesman Jim Davidson said the company helps schools provide relevant information to students who have chosen to receive that information. Students can opt out of Web tracking by contacting schools directly, he said.
Doug Mell, a spokesman for UW-Stout, said in an email that the school used Capture's Web tracking for a one-year trial and did not renew the contract this year. The female student who was tracked last year voluntarily gave the school her background information when she applied, he said. She enrolled in the school last year.

Consultants are expanding their influence on college campuses. Ruffalo Noel Levitz, based in Cedar Rapids, Iowa, has hired the top admissions officers at more than two dozen universities — including Vanderbilt, Creighton and Marquette — to do paid consulting work on the side, according to interviews and records. Some university officials received compensation from Ruffalo Noel Levitz at the same time that their schools were paying customers of the company — raising questions about potential conflicts of interest, Thacker said.

The vast majority of universities reviewed by The Post do not tell students the schools are collecting their information. In a review of the online privacy policies of all 33 schools using Web tracking software, only three disclosed the purpose of the tracking.

The other 30 omitted any explanation or did not explain the full extent or purpose of their tracking.

The State University of New York's College of Environmental Science and Forestry said in its online privacy policy that it "does not use cookies." However, a representative from the school said in an email that the school does use Capture Higher Ed's tracking cookies to show relevant pop-up ads to students but deletes the cookies from its databases "within four hours."
Some privacy experts say colleges' failure to disclose the full extent of how they share data with outside consultants may violate the spirit if not the letter of the Family Educational Rights and Privacy Act, or FERPA, a federal law protecting the privacy of student education records at schools that receive federal education funds. FERPA generally requires that schools ask for students' permission before sharing their personal data with any outside parties.

Rather than getting permission, some schools have classified the consulting companies as "school officials," a legal designation that exempts them from FERPA if certain conditions are met.

Zachary Greenberg, a program officer at the Foundation for Individual Rights in Education, a student advocacy group, said colleges that do this risk undermining one of the goals of FERPA — to make the management of records more transparent. "Students deserve to know where their information is going," Greenberg said.

The Education Department can suspend all federal funding to any school it finds in violation of FERPA but has never imposed that penalty in the 45 years since the law was created. The agency has other enforcement measures and works with offenders to voluntarily come into compliance, said Angela Morabito, a spokeswoman for the Education Department. She declined to say whether colleges may be violating the law by sharing data with consulting companies.

Many schools do not give students the ability to opt out of data collection. Jacquelyn Malcolm, chief information officer at the State University of New York's Buffalo State College, said that if prospective students do not want their Web browsing tracked, they should not visit her school's website.
"You have a choice of not interacting at all," Malcolm said in an interview, adding that applicants can get information by calling the school, visiting its social media accounts or visiting other websites with information about different colleges.
In an email, a spokesman for SUNY Buffalo State later said that the school is exploring new ways to inform students about its privacy practices and that anyone can request not to be tracked by sending an email directly to Malcolm.

recruits with socioeconomic data
Data tools appeal to schools that are trying to increase revenue by recruiting students who can afford to pay tuition.

At Mississippi State University, a state school with more than 18,000 undergraduates, administrators use data to filter a large number of potential applicants down to a select pool of recruits who are a good fit for the school's academic programs and do not need much financial aid.

Students/parents Dept Educ

Each year, Mississippi State buys data on thousands of high school students from testing firms including the College Board, which owns the SAT, said John Dickerson, assistant vice president for enrollment. These students all gave permission to have their data shared by checking a box when they took the SAT. The nonprofit testing company says on its websitethat it licenses the names and data of each student for 47 cents apiece.
Next, Mississippi State shares its list of prospects with Ruffalo Noel Levitz, which uses a formula to assign each one a score. According to Dickerson, the formula for out-of-state students gives the most weight (30 percent) to a student's desired major; someone choosing agriculture or veterinary sciences, areas where the school is strong, will score higher than a student who wants to major in music. The formula also weighs their distance from campus (7.9 percent), income level (7.2 percent) and consumer purchasing behavior (6.8 percent), among other factors.

The formula is an example of predictive analytics, a field of computer science that attempts to predict the likelihood of future events by looking for patterns in data. Similar to software that tries to predict what movies or music someone will like, these formulas attempt to guess which students are a good match for a college based on how many attributes they have in common with students who previously enrolled in the school.

A predictive formula may also be adjusted to favor the types of people a college wants more of, such as ethnic minorities or students of financial means. Mississippi State uses socioeconomic data in its admissions algorithm to recruit more high-income students from outside the state, Dickerson said. Like many public universities, Mississippi State has ramped up out-of-state recruiting because those students pay higher tuition. The university drew 42 percent of its freshmen from out of state in 2018, up from 26 percent a decade earlier, federal data shows.
"From a practical standpoint," Dickerson said, "you would want to know if folks have an ability to pay."

The vast majority of Mississippi State students still receive some form of financial aid, and the school says it does not use financial information to determine who gets an offer of admission. However, focusing recruiting resources on higher-

income students means lower-income students may receive less encouragement to apply for college.

Shaquilla Wordlaw, a junior at Mississippi State, said she thinks it is a good idea for college recruiters to use more data to target messages to the right students. But Wordlaw, who is from Starkville, where Mississippi State is based, says the school should not discriminate against students based on their income.

"They're choosing those who are a part of the upper class rather than middle or lower, because they want money," Wordlaw said. "They're not focused on the education they are providing."

Consulting companies may estimate a student's financial position by checking their Zip codes against U.S. Census data for estimated household incomes in that area. Ruffalo Noel Levitz and Capture Higher Ed also buy information from third-party data brokers, which gather consumer data from public and private databases on property holders, magazine subscribers and supermarket loyalty-card members.

Some schools say data analysis can help them find students who might not have applied in the first place. George Mason University, in Northern Virginia, uses data analysis tools to look for nontraditional prospects who might have working-class parents or be the first in their family to go to college, said David Burge, the school's vice president for enrollment management.

Consulting companies woo college officials

As they pursue student data, colleges have embraced an industry of consultants. Hundreds of school administrators filled the ballroom of a Nashville convention center in late July for a keynote speech by Sumit Nijhawan, a former tech executive who became CEO of Ruffalo Noel Levitz last year. He paced before a large screen and discussed how data is helping colleges tailor their pitch to individual students, similar to how tech companies such as Spotify and Netflix surface music and videos based on the user, he said. "Usually the solution to problems is lurking somewhere around in data," Nijhawan told the crowd. "And there's a lot of data in higher ed — no doubt about that."

The three-day conference, replete with lunch buffets, PowerPoint presentations and free coffee mugs with company logos, was an example of how consulting companies are trying to win over school officials as they negotiate for larger contracts and more access to student data.

At least 30 admissions officers have taken part in Ruffalo Noel Levitz's associate consulting program over the past decade, according to interviews and records posted on the company's website. Emails reviewed by The Post show the program is helping Ruffalo Noel Levitz build closer ties to campus decision-makers.

Cecilia Castellano, vice provost of strategic enrollment planning at Bowling Green State University in Ohio, became an associate consultant for Ruffalo Noel Levitz around the same time her school signed a three-year, $48,000 contract, which was obtained by The Post through a public-records request. Castellano, who was listed as the "primary contact" on that business deal in October 2016, received emails from Ruffalo Noel Levitz a few days later, asking her to sign up for a "new associate training workshop" later in the year.

In an email to Castellano the same year, Ruffalo Noel Levitz asked her to help pitch a $13,590-per-person certification program to potential customers. "Please encourage the teams on your client campuses to consider the program," the email said.

Dave Kielmeyer, a university spokesman, said Castellano attended the consultant training in 2016 and has since done two paid consulting projects for the company. She got approval from the school, which did not see the work as a conflict, Kielmeyer said. Castellano "has a role in hiring vendors," he said, but the school's provost or chief financial officer must approve consulting contracts.

Admissions officers at Vanderbilt, Creighton and Marquette universities say that they have disclosed their consulting roles with their colleges and are careful not to work with competing schools. Nijhawan, the Ruffalo Noel Levitz CEO, said in an interview that the program is aimed at helping school administrators "share knowledge across the industry."

Matching 'cookies' to student identities

Some of the same technologies that big companies use to track users and show ads to consumers are gaining traction in college admissions. One example is Capture Higher Ed's behavioral tracking service, which relies on cookies to record every click students make when they visit a university website.

Each visitor to the university site gets a cookie, which sends Capture information including that person's Internet protocol address, the type of computer and browser they are using, what time of day they visited the site and which pages within the site they clicked on, according to Patrick Jackson, chief technology

officer for digital privacy firm Disconnect, who reviewed college websites on behalf of The Post.

Every time that person returns to the site, Capture learns more information about them, such as their interest in athletics or the amount of time they spend on financial aid pages, according to promotional videos on the company's website. Initially, the cookies identify each visitor by the IP address, a unique code associated with a computer's Internet connection, but Capture also offers software tools to match the cookie data with people's real identities, according to the company's promotional videos. Colleges do this by sending marketing emails to thousands of prospective students, inviting them to click on a hyperlink inside the message for more information about a particular topic, according to the videos.

When a student clicks on the link, Capture learns which email address is associated with which IP address, connecting the student's real identity to the college's snapshot of the student's Web browsing history, Capture executives said in one of the videos.

Promotional video for Capture Higher Ed's student tracking service.

"We are embedding links in every email," Billy Pierce, then director of undergraduate admission at the University of Toledo, a Capture customer, said onstage at a college admissions conference in 2016. "You want more of the identified visitors coming to your website because those are the kids that you have their name, their address, their email, sometimes their phone number — any information you have in your system now gets tied to their behavior," Pierce said at the conference, a video of which was posted to YouTube.

Meghan Cunningham, a spokeswoman for the University of Toledo, said the school uses Capture's software code on its website and in some — not all — of its marketing emails in an effort to give students information relevant to them. In an email, Pierce added that students choose to give their names and contact information to the school.

Admissions officers say behavioral tracking helps them serve students in the application process. When a college sees that a qualified student is serious about applying based on the student's Web behavior, it can dedicate more staffers to follow up.

"An admissions counselor may only have an hour in a given day to make contact with prospective students," Chrissy Holliday, vice president of enrollment at Colorado State University at Pueblo — a Capture Higher Ed client — said in an email. "The web data allows the counselor to know which students are currently most engaged and might benefit most from that contact."

But Web tracking may unfairly provide an advantage to students with better access to technology, said Bradley Shear, a Maryland lawyer who has pushed for better regulation of students' online privacy. A low-income student may be a strong academic candidate but receive less attention from recruiters because the student does not own a smartphone or have high-speed Internet access at home, he said.

"I don't think the algorithm should run the admissions department," Shear said.

The Washington Post
Democracy Dies in Darkness

Colleges need to be transparent about the personal data they collect

By **Letters to the Editor**

Oct. 18, 2019 at 5:29 p.m. EDT

The Oct. 15 front-page article "Colleges use Web data to rank students — before they apply" detailed how colleges are building virtual libraries of personal data in the interest of finding the applicants most likely to enroll and pay tuition.

Colleges should disclose their use of tracking software, cookies, analytics and predictive scores. At a bare minimum, potential applicants should be told on admissions materials what information is collected about them, from what sources and how it will be considered in the application process.

Disclosures should be clear. Saying a college uses "publicly available information" or "Internet activity" in its admissions decisions isn't good enough. Students need to know whether their browsing patterns, email open rates or time spent on a college's website affect their likelihood of being admitted.

Higher-education leaders should ensure prospective students know what information is collected about them and how it is used to make decisions about their academic future.

Sara Collins, Washington

The writer is a policy counsel for the Future of Privacy Forum.

Read more letters to the editor.

The Washington Post

Technology

School apps track students from classroom to bathroom, and parents are struggling to keep up

+ Add to list

A digital hall-pass app that tracks bathroom trips is the latest school software to raise privacy concerns

By Heather Kelly
October 29, 2019

When Christian Chase wants to take a bathroom break at his high school, he can't just raise his hand.

Instead, the 17-year-old senior makes a special request on his school-issued Chromebook computer. A teacher approves it pending any red flags in the system, such as another student he should avoid out in the hall at the same time, then logs him back in on his return. If he were out of class for more than a set amount of time, the application would summon an administrator to check on him.

Heritage High School in Loudoun County, Va., introduced the software, called e-Hallpass, in September as a way to track trips to the bathroom, the nurse's office, the principal or other places on campus. It collects the data for each student's comings and goings so approved administrators can see pass histories or look for patterns.

I just think it's a violation of our privacy, and I don't think it's omething that needs to be in place. I would understand if it was omething for specific people or even underclassmen," said Chase, vho started an online petition on Change.org to remove the echnology he calls invasive.

As technology becomes more pervasive in schools, parents and tudents are getting a lesson in data privacy. Every year, they face he overwhelming task of sorting through the benefits, drawbacks nd privacy implications of each piece of educational software. 'amilies have to decide if they are comfortable with how nformation is being collected and used and whether they want to - or even can — opt their kids out.

Hundreds of applications, big and small, are being used at schools

across the country to do everything from track homework to modify behavior. They can collect data about intelligence, disciplinary issues, personalities and schedules.

It is common for families to take precautions outside of school, enforcing screen time rules at home and limiting what photos they post of their children on social media. But controlling what happens at school is harder, in part because districts are not required to inform parents of every type of software students use. And the apps, as well as the schools deploying them, have different rules for how they use, share and store data.

There are classroom management tools like Google's G Suite for Education that tracks school work and helps teachers, parents and students communicate via messaging and email. Smaller apps such as ClassDojo, which claims to be in use at 90 percent of K-8 schools in the United States, tackle specific subjects or problems. That app lets teachers communicate with parents and grant students virtual points for positive behaviors like teamwork or subtract them for negative actions like being out of their chair. Newer "personalized learning" programs attempt to develop custom education plans for students based on data they collect about their interests and skills.

Google, ClassDojo and E-Hallpass say in their privacy policies that student data is not shared with third-party companies for marketing or advertising, and parents can request deletion. E-Hallpass says schools are entirely in charge of the data the program collects and can delete it as often as they like.

Advocates for using these types of software say they can revolutionize education, helping students gain valuable skills to prepare them for college and then the workplace. Research on the technology is still in the early stages.

Still, privacy advocates say parents face a conundrum. Though there have been some improvements, the education technology industry as a whole is still lagging in privacy protections, with many apps still selling easily de-anonymized data and tracking users, said Girard Kelly, counsel and director of privacy review at Common Sense Media, a nonprofit organization that reviews technology and media targeting young people.

School districts increasingly have their own data privacy agreements for third-parties, but with anywhere from 200 to 600 applications being used across all schools and grades in a single district, by Kelly's estimate, screening every classroom tool can be

difficult.

As a result, families are often left on their own trying to navigate a co[illegible]sing maze of privacy agreements, school policies and federal privacy regulations.

"Everyone feels overwhelmed, everyone feels like they don't know what they're doing, and that's because the technology is not transparent and does not allow for easy understanding of what your kid is using," said Monica Bulger, a research affiliate at the independent, nonprofit Data and Society Research Institute.

It is reflective of a broader distrust in big tech. According to a Pew Research Center survey last year, only a quarter of Americans think tech companies "do enough to protect the personal data of their users."

Some parents do manage to comb through privacy policies, opt-out of classroom programs and ask to have students' data wiped from company servers — even when it puts them at odds with their kids' own schools.

K[illegible]in Phatak was recently notified her 11th-grader was using a program called Thrively, which asks students to take a personality

ıssessment and then uses the answers to determine their strengths," recommending careers or skills they should learn.

Her son had already used it once. so Phatak asked her school at the Sweetwater Union High School District in Chula Vista, Calif., to opt ıim out, to see a copy of the data the company collected about him ınd for the company to delete any information about him. First, the ›rincipal suggested she speak with Thrively's CEO so he could lirectly address her concerns.

As a parent, why am I having to go through this? Why is the rincipal of our school on a first-name basis with the CEO of a ompany who is collecting data about our kids?" said Phatak. She ventually received a copy of the data and was told it was deleted, ut then her child's teacher accidentally had him use the tool again.

weetwater school officials did not reply to repeated requests for ›mment. Thrively's CEO Girish Venkat said the incident was an nomaly, but that he does try to talk to parents who request that ıeir kids' data be deleted. Of the four parents who have asked, he ays all but one decided to let their kid keep using Thrively. The ›ol is used by roughly 1 million kids, he added.

hrively's privacy policy says it does not sell or rent user data, but

like many education apps, it can use depersonalized and aggregated information to market products to parents.

"Many parents are upset about the lack of privacy involved with the data going into private corporate hands and how their education is being outsourced to tech companies," said Leonie Haimson, head of Parent Coalition for Student Privacy, an advocacy group that gives parents guidance on navigating school data issues.

She recommends making an appointment with a teacher or school principal to ask questions, including what programs are in use, who has access to the data, if the companies are barred from using the information for marketing and if the programs are in compliance with state and federal privacy laws.

Federal laws put some limits on how software is used by schools. The Family Educational Rights and Privacy Act of 1974 limits how schools can share educational records and gives parents the right to review them. The Children's Online Privacy Protection Act has rules that apply to companies collecting data about kids under 13. However, under the law, schools can consent on behalf of parents for educational products. The Federal Trade Commission is considering updating COPPA.

'arents also have rights under the Protection of Pupil Rights
mendment, which requires schools to get parental permission for
ny federally funded student survey or sensitive topic evaluations,
uch as religion, political views or income. But for the most part,
chools are not legally obligated to get permission from parents to
se specific software in classrooms, or to let students opt out.

ome schools, like those in the Montgomery County public school
istrict in Rockville, Md., are more receptive to parents policing
heir children's technology. Ellen Zavian, a lawyer and professor at
eorge Washington University Law School, has cleared her middle-
chool aged son to use Google's education software, but not
lassDojo.

At the beginning of every school year I send the principal what my
on's allowed to be on and what he's not allowed to be on, and thus
ar my local schools have been incredibly supportive and have been
illing to learn from me as I have been willing to learn from them,"
avian said. "My goal is to give my child the smallest footprint
ossible, to give him the largest opportunity possible."

o help parents and educators make decisions, Common Sense
edia examines education-technology privacy policies and looks at
ctors such as whether data is sold to third parties or if the apps

include ads. An application might be dinged for not saying whether it tracks users or created ad profiles, and get points for storing data securely. (The project is funded by the Bill and Melinda Gates Foundation, which is invested in edTech, and Facebook CEO Mark Zuckerberg's philanthropic organization, The Chan Zuckerberg Initiative, which makes the personalized learning program Summit Learning.)

Common Sense Media found both ClassDojo and the stand-alone Google Classroom tool to have sufficient privacy policies — enough to get a green check mark and a "Use responsibly" label — meaning they met the organization's minimum privacy requirements. Points were subtracted from ClassDojo's overall score for its system for obtaining parental consent, while Google Classroom was dinged for how much data it collected.

ClassDojo said its tool is designed to collect the bare minimum amount of information about students and to not create a digital footprint, and that it goes "above and beyond" for parental consent. Google said student information collected by G Suite for Education products like Google classroom is only used to provide the services themselves, and that schools are in control of how often it is deleted.

E-Hallpass does not have a rating by Common Sense Media yet, though the company that makes it, Eduspire Solutions, says it is used in hundreds of schools in the United States. Eduspire President Brian Tvenstrup says the system is meant to keep track of students in an emergency, decrease vaping, identify vandals and crack down on truancy. A feature that lets a school flag specific students or groups who should not be in the hallways at the same time can cut down on bullying or gang violence, Tvenstrup said.

Students can also choose to use e-Hallpass on their personal

martphones, and the mobile app does not use GPS tracking.

oth e-Hallpass and its competitor SmartPass Mobile say another elling point is that the physical objects many classes have typically sed for hall passes are unsanitary. A computerized system cuts out he germs.

s for privacy concerns, Tvenstrup says the same information was lready being collected by schools — just on paper. Schools have ontrol over how long they store the data. Some delete it annually, few delete more often than that.

In our case we're providing a service. It's a database of sorts, but 's analogous to the transition of other digital record keeping that chools keep," Tvenstrup said. "Twenty-five years ago, grades were ot digitized."

Many students and parents see a digital hall-pass program ifferently. At Heritage High School, Chase says, other students are lso unhappy about the new system. The Change.org petition he reated has more than 400 signatures, though it is not clear how nany of them attend the school, which has around 1,500 students.

he Loudoun County Public School district, where Heritage High chool is located, allows parents to opt their kids out of the e-allpass system and use alternative passes instead, according to Vayde Byard, the school district's public information officer. It eletes the data it collects once a year, and the more advanced eatures like cross-referencing students are not widely used in the istrict. The system is in use at 23 middle and high schools across ne district, and each school makes its own decisions about which eachers and administrators can see the data for all kids.

orthwood High School, in Montgomery County, Md., plans to ring e-Hallpass to its campus at the end of October, though a

number of parents planned to oppose the decision at a recent PTA meeting. The school will have a single school-issued computer in each class where students can request passes and will not use it on personal cellphones, according to Derek Turner, head of communication for Montgomery County Public Schools. The district does not have plans to test it at other schools, Turner said.

Both the Montgomery and Loudon County school districts have data privacy agreements tech companies must agree to as part of their contracts. When online educational tools are used without contracts, the schools say they vet and approve them.

Privacy attorney Brad Shear has two elementary-age kids in the Montgomery County schools. He has been vocal about parental privacy rights and successfully lobbied the district to adopt an annual "data deletion week." Now, the school purges any unnecessary data about students from tools like Google's education suite, keeping essential information such as grades.

RIDE

However, if the district does decide to test e-Hallpass in more schools, Shear and other parents are ready to mobilize against it.

"I will not allow this app to be utilized in my kids' schools, period. If the app ends up getting rolled out I will make sure that I get the PTA involved," Shear said. "This is bathroom big brother."

Heather Kelly
Heather Kelly is a reporter covering the ways technology affects everyday life. Based in San Francisco, she joined The Washington Post in 2019 after seven years at CNN, where she worked as a writer and editor covering consumer technology trends and Silicon Valley. Follow

https://www.shearlaw.com/marylands-student-data-privacy-act-of-2015/ 2015

Last fall, California enacted what Education Week called a "landmark" student-data privacy law (SB 1177). This was passed because some educational technology companies were caught abusing their access to personal student data.

As a parent, the digital privacy of my children is very important. I don't want an educational technology vendor using my kids' school created digital data for behavioral advertising or for profiling purposes that may be utilized to discriminate against them in the future. The Family Educational Educational Rights and Privacy Act (FERPA) was enacted in 1974 and has not kept up with the innovative digital learning technologies that are becoming more widely available for our students.

Today, schools utilize cloud-based technologies, apps, and other digital services to teach our children. Unfortunately, metadata created from these platforms is not considered an educational record under FERPA and thus not protected from the prying eyes of advertisers and others who covet this rich information. Therefore, students and their families need stronger legal privacy protections. Absent more robust student privacy laws, our children's privacy and safety will be compromised and innovative learning and educational technologies will face increased parent skepticism and opposition.

Maryland, a state that has vied with California to be a national leader in digital privacy protection recently introduced the Student Privacy Act of 2015. The bill is modeled after California's groundbreaking SB 1177. Mark Schneiderman, senior director of education policy for the Software & Information Industry Association said California's SB 1177 "seems to generally strike the right balance". Thus, the SIIA should hold the same position on Maryland's student data privacy act.

Last month, President Obama gave a historic speech at the FTC about his privacy agenda for the last two years of his term. In regards to student privacy the President stated: *"But we've already seen some instances where some companies use educational technologies to collect student data for commercial purposes, like targeted advertising. And parents have a legitimate concern about those kinds of practices.*

So, today, we're proposing the Student Digital Privacy Act. That's pretty straightforward. We're saying that data collected on students in the classroom should only be used for educational purposes -— to teach our children, not to market to our children. We want to prevent companies from selling student data to third parties for purposes other than education. We want to prevent any kind of profiling that outs certain students at a disadvantage as they go through school."

Congress is also concerned about student privacy issues. On February 12, 2015, it held a hearing entitled, "How Emerging Technology Affects Student Privacy". The testimony during the hearing demonstrated that FERPA needs to be updated. While my hope is that one day

Congress passes stronger student privacy legislation, I am not optimistic in the short term due to all of the acrimony on Capitol Hill.
Until this occurs, states such as Maryland must fill this void and step up to protect the digital privacy and cyber security of our kids.

While it doesn't go into effect until 2020, the California Consumer Privacy Act represents one of the most sweeping acts of legislation enacted by a U.S. state to bolster consumer privacy. Falling on the heels of the GDPR, California Consumer Privacy Act may mark the beginning of stricter U.S. consumer privacy protections.

CALIFORNIA CONSUMER PRIVACY ACT EXPLAINED

The California Consumer Privacy Act is a piece of consumer privacy legislation which passed into California law on June 28th of 2018. The bill, also known as "AB 375," has been described by some as "almost GDPR in the US." Far and away, this Act is the strongest privacy legislation enacted in any state at the moment, giving more power to consumers in regards to their private data. With a variety of major tech giants based in California, including Google and Facebook (both of which have recently suffered data breaches), AB 375 is poised to have far-reaching effects on data privacy. AB 375 will go into full effect on January 1st, 2020. Companies that already comply with the GDPR may find that they currently meet many of the requirements set forth in the California Data Privacy Protection Act. With many experts predicting that other states will follow suit in the coming years, companies across the U.S. that take proactive steps today to better protect consumer data will be best equipped to ride the waves of change.
All fifty states have enacted legislation to protect consumers' private information, but some states have more stringent laws and penalties than others. To learn about data protection laws in your state, read through the Definitive Guide to US State Data Breach Laws or view the United States Data Breach Heatmap infographic.

KEY TERMS OF THE PRIMARY CALIFORNIA CONSUMER PRIVACY ACT DEFINED

There are a number of terms defined in the legislation in order to clarify the parameters of the law. Certain businesses and all Californian consumers are the two groups who fall under the provisions in the bill, defined as:

- Consumer: According to the Act, "'Consumer' means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations..."
- Business: This term has a lengthy definition in the bill, which describes many typical business models and types. Three key articles to pay attention to include:

- For-profit entities which do business in California and collect personal information of consumers.
- "Has annual gross revenues in excess of twenty-five million dollars ($25,000,000)..."
- "Derives 50 percent or more of its annual revenues from selling consumers' personal information."

DEFINING "PERSONAL INFORMATION"

Another important term loosely defined in the bill is "personal information." According the AB 375, "The bill...would define 'personal information' with reference to a broad list of characteristics and behaviors, personal and commercial, as well as inferences drawn from this information."

Dozens and perhaps hundreds of specific data items are mentioned in the legislation, including:

- Biometric data
- Household purchase data
- Family information (e.g., how many children)
- Geolocation
- Financial information
- Sleep habits

WHAT DOES THE CALIFORNIA CONSUMER PRIVACY ACT PROVIDE FOR CONSUMERS?

- General Disclosure: If a business (as defined by the bill) collects any type of personal information, this should be disclosed in a clear privacy policy available on the website of the business.
- Specific Requests: Should a consumer desire to know what data is being collected, the company is required to provide such information — specifically about the individual. Some of the requests that can be made include:

- The categories of personal information collected
- Specific data collected about the individual
- Methods used to collect the data
- A business' purpose for collecting the information
- Third parties to which personal information may be shared

- Deletion: If the consumer desires, personal information (with exceptions) will be deleted by the business.
- Same Service: Regardless of a consumer's request and preferences about how their personal information is handled, businesses are required to provide "equal service and pricing...even if they [consumers] exercise their privacy rights under the Act."

HOW TO COMPLY WITH THE CALIFORNIA CONSUMER PRIVACY ACT

As it stands, businesses will be required to comply with any and all provisions outlined in the final version of AB 375 by January 1, 2020. Companies actively doing business in California will need to adjust their current practices to avoid violations of the law.
Many of these changes translate to a need for:

- Organized Data Collection: The bill allows consumers to request the specific information collected about them. These requests are to be provided at no cost to the consumer. Companies need to have the ability to quickly search, compile and send these reports to consumers.
- Clear, Transparent Policies: Consumers can request a report on the types of data collected, data sources, collection methods, and uses for their data. While the data itself needs to be stored in a well-constructed database, many consumer questions can be quickly answered in comprehensive privacy and data collection policies.
- Knowledge of Specific Provisions: There are clearly outlined requirements within the California Data Privacy Protection Act including things such as:

- "Provide a clear and conspicuous link on the business' Internet homepage, titled 'Do Not Sell My Personal Information,' to an Internet Web page..."

- Ensure any individuals who handle consumers' private data know and understand all pertinent regulations.

  In the time leading up to full implementation in 2020, there will likely be amendments that change current provisions, remove requirements, or even add to the regulation. It is important for all businesses to work towards a safe and healthy relationship between data collection and privacy while staying up-to-date regarding new data regulations.

  The General Data Protection Regulation (GDPR), agreed upon by the European Parliament and Council in April 2016, will replace the Data Protection Directive 95/46/ec in Spring 2018 as the primary law regulating how companies protect EU citizens' personal data. Companies that are already in compliance with the Directive must ensure that they are also compliant with the new requirements of the GDPR before it becomes effective on May 25, 2018. Companies that fail to achieve GDPR compliance before the deadline will be subject to stiff penalties and fines.
  GDPR requirements apply to each member state of the European Union, aiming to create more consistent protection of consumer and personal data across EU nations. Some of the key privacy and data protection requirements of the GDPR include:

- Requiring the consent of subjects for data processing
- Anonymizing collected data to protect privacy
- Providing data breach notifications
- Safely handling the transfer of data across borders
- Requiring certain companies to appoint a data protection officer to oversee GDPR compliance

Noel Levitz and Capture Higher Ed also buy information from third-party data brokers, which gather consumer data from public and private databases on property holders, magazine subscribers and supermarket loyalty-card members.

Some schools say data analysis can help them find students who might not have applied in the first place. George Mason University, in Northern Virginia, uses data analysis tools to look for nontraditional prospects who might have working-class parents or be the first in their family to go to college, said David Burge, the school's vice president for enrollment management.

Consulting companies woo college officials

As they pursue student data, colleges have embraced an industry of consultants. Hundreds of school administrators filled the ballroom of a Nashville convention center in late July for a keynote speech by Sumit Nijhawan, a former tech executive who became CEO of Ruffalo Noel Levitz last year. He paced before a large screen and discussed how data is helping colleges tailor their pitch to individual students, similar to how tech companies such as Spotify and Netflix surface music and videos based on the user, he said. "Usually the solution to problems is lurking somewhere around in data," Nijhawan told the crowd. "And there's a lot of data in higher ed — no doubt about that." The three-day conference, replete with lunch buffets, PowerPoint presentations and free coffee mugs with company logos, was an example of how consulting companies are trying to win over school officials as they negotiate for larger contracts and more access to student data.

At least 30 admissions officers have taken part in Ruffalo Noel Levitz's associate consulting program over the past decade, according to interviews and records posted on the company's website. Emails reviewed by The Post show the program is helping Ruffalo Noel Levitz build closer ties to campus decision-makers.

Cecilia Castellano, vice provost of strategic enrollment planning at Bowling Green State University in Ohio, became an associate consultant for Ruffalo Noel Levitz around the same time her school signed a three-year, $48,000 contract, which was obtained by The Post through a public-records request. Castellano, who was listed as the "primary contact" on that business deal in October 2016, received emails from Ruffalo Noel Levitz a few days later, asking her to sign up for a "new associate training workshop" later in the year.

In an email to Castellano the same year, Ruffalo Noel Levitz asked her to help pitch a $13,590-per-person certification program to potential customers. "Please encourage the teams on your client campuses to consider the program," the email said.

Dave Kielmeyer, a university spokesman, said Castellano attended the consultant training in 2016 and has since done two paid consulting projects for the company. She got approval from the school, which did not see the work as a conflict, Kielmeyer said. Castellano "has a role in hiring vendors," he said, but the school's provost or chief financial officer must approve consulting contracts.

Admissions officers at Vanderbilt, Creighton and Marquette universities say that they have disclosed their consulting roles with their colleges and are careful not to work with competing schools. Nijhawan, the Ruffalo Noel Levitz CEO, said in an interview that the program is aimed at helping school administrators "share knowledge across the industry."

Matching 'cookies' to student identities

Some of the same technologies that big companies use to track users and show ads to consumers are gaining traction in college admissions. One example is Capture Higher Ed's behavioral tracking service, which relies on cookies to record every click students make when they visit a university website.

Each visitor to the university site gets a cookie, which sends Capture information including that person's Internet protocol address, the type of computer and browser they are using, what time of day they visited the site and which pages within the site they clicked on, according to Patrick Jackson, chief technology officer for digital privacy firm Disconnect, who reviewed college websites on behalf of The Post.

Every time that person returns to the site, Capture learns more information about them, such as their interest in athletics or the amount of time they spend on financial aid pages, according to promotional videos on the company's website.

Initially, the cookies identify each visitor by the IP address, a unique code associated with a computer's Internet connection, but Capture also offers software tools to match the cookie data with people's real identities, according to the company's promotional videos. Colleges do this by sending marketing emails to thousands of prospective students, inviting them to click on a hyperlink inside the message for more information about a particular topic, according to the videos.

When a student clicks on the link, Capture learns which email address is associated with which IP address, connecting the student's real identity to the college's snapshot of the student's Web browsing history, Capture executives said in one of the videos.

Promotional video for Capture Higher Ed's student tracking service.

"We are embedding links in every email," Billy Pierce, then director of undergraduate admission at the University of Toledo, a Capture customer, said onstage at a college admissions conference in 2016. "You want more of the identified visitors coming to your website because those are the kids that you have their name, their address, their email, sometimes their phone number — any information you have in your system now gets tied to their behavior," Pierce said at the conference, a video of which was posted to YouTube.

Meghan Cunningham, a spokeswoman for the University of Toledo, said the school uses Capture's software code on its website and in some — not all — of its marketing emails in an effort to give students information relevant to them. In an email, Pierce added that students choose to give their names and contact information to the school.

Admissions officers say behavioral tracking helps them serve students in the application process. When a college sees that a qualified student is serious about applying based on the student's Web behavior, it can dedicate more staffers to follow up.

"An admissions counselor may only have an hour in a given day to make contact with prospective students," Chrissy Holliday, vice president of enrollment at Colorado State University at Pueblo — a Capture Higher Ed client — said in an email. "The web data

allows the counselor to know which students are currently most engaged and might benefit most from that contact."

But Web tracking may unfairly provide an advantage to students with better access to technology, said Bradley Shear, a Maryland lawyer who has pushed for better regulation of students' online privacy. A low-income student may be a strong academic candidate but receive less attention from recruiters because the student does not own a smartphone or have high-speed Internet access at home, he said.
"I don't think the algorithm should run the admissions department," Shear said.